Manuel d'utilisation

Middleware eID v2.5 pour GNU/Linux

© 2006 SPF Technologie de l'Information et de la Communication (Fedict)

Table des matières

Introduction....3
Installation....4
Installation à partir du code source....4
Installation de paquets de distribution spécifiques....5
Exigences système après installation....5
Les éléments du logiciel eID....6
Le Filtre Vie privée....7
Le module PKCS#11....9
Application pour lire et contrôler la carte....10
Les Outils de la Ligne de commandes....15

© 2006 SPF Technologie de l'Information et de la Communication (Fedict)

INTRODUCTION

A mi-2006, le nombre de cartes d'identité électronique ou eID atteignait déjà 2 millions et demi, et il s'en ajoute chaque année autant. De plus en plus de services publics et d'entreprises proposent de nouveaux services Internet et programmes qui utilisent l'eID.

Pour employer l'eID avec ces services et programmes, vous avez besoin d'un lecteur de carte et d'un logiciel spécial – le *middleware* (ou “logiciel médiateur”) *eID* – pour lire la carte. Les lecteurs de carte sont disponibles dans les magasins informatiques traditionnels et dans les grandes surfaces. Le middleware eID est mis à disposition de tous, par le service fédéral, sur le portail fédéral http://www.eid.belgium.be.

Avec le middleware eID, vous pouvez lire et sauvegarder le contenu de la carte d'identité, enregistrer automatiquement votre carte d'identité dans Linux et l'utiliser avec des programmes répandus comme OpenOffice, Firefox, Thunderbird, Adobe Reader, Lotus Notes, etc.

Outre votre identité, adresse et photo, la puce électronique insérée dans la carte contient également des clés cryptographiques qui sont utilisées par ces programmes pour prouver votre identité ou pour apposer une signature électronique sur un document informatique.

Pour plus d'information sur la LSB, consultez http://www.freestandards.org/en/Specifications

Le middleware eID est adapté aux versions suivantes de Linux:

- kernel v2.6
- PC/SC Lite 1.2 ou 1.3
- de préférence conforme à la Linux Standards Base v 3.1

Ce manuel est destiné à des utilisateurs ordinaires. Il contient une description des différents éléments du logiciel et de leur fonction. Il explique également comment installer et utiliser ce logiciel. Les informations figurant dans ce document s'appliquent au version 2.5 du middleware eID.

Des informations additionnelles pour les utilisateurs professionnels, les administrateurs système et les programmeurs sont disponibles dans des notes techniques séparées. Outre ce manuel et ces notes techniques, les programmeurs ont également intérêt à consulter la documentation du eID Software Development Kit.

© 2006 SPF Technologie de l'Information et de la Communication (Fedict)

INSTALLATION

INSTALLATION À PARTIR DU CODE SOURCE

Pour une installation à partir du code source, le logiciel suivant doit déjà être installé:

- Qt 3.3.x libraries + header files
- OpenSSL 0.9.x libraries + header files
- gcc
- Python
- pkgconfig
- LSB core package
- PC/SC Lite 1.2.x ou 1.3.x daemon, libraries et header files
- Scons (optionnel)
- Java2 SDK v1.4 ou 1.5 (optionnel)
- wxGtk 2.6 libraries + header files (optionnel)

Une séquence d'installation typique sur une distribution Linux moderne à base de noyau (core package) LSB se présente comme suit:

```
# ./configure
# make
# su
enter your password:
# make install
# ldconfig /usr/local/lib
# /usr/lib/lsb/install_initd /etc/init.d/belgium.be-beidpcscd
# /usr/lib/lsb/install_initd /etc/init.d/belgium.be-beidcrld
```

Si la distribution ne possède pas de base de noyau LSB vous devez effectuer les deux dernières étapes (l'enregistrement des scripts init) selon les règles de votre distribution.

Vous trouverez des informations complémentaires dans les fichiers README et INSTALL livrés avec le code source. INSTALL renseigne également une marche à suivre générale pour l'installation correcte de scripts init pour les 2 daemons (démons) beidpcscd et beidcrld.

L'archive tar (tarball) avec le code source contient aussi une icône qui peut être utilisée pour le menu Start du desktop manager (KDE, Gnome, ...).

INSTALLATION DE PAQUETS DE DISTRIBUTION SPÉCIFIQUES

Certaines distributions Linux offrent des paquets prêts à l'emploi du logiciel eID dans le format de paquet standard (rpm, dev, ...) pour cette distribution.

Utilisez le gestionnaire de paquets de votre distribution et installez les paquets suivants:

- eID middleware (cherchez sur "beid", "Belgium", "eID", ...)
- PC/SC Lite
- LSB Core
- wxWidgets (wxGTK) 2.6
- OpenSSL
- Qt 3.3.x
- Java Runtime environment (optionnel)

Il est possible que le middleware eID ait été fractionné en plusieurs paquets par les responsables de la distribution. Cette répartition peut être différente d'une distribution à l'autre.

EXIGENCES SYSTÈME APRÈS INSTALLATION

Le daemon pcscd du paquet PC/SC Lite doit être démarré via un script init dans /etc/init.d. Sans ce démon, le middleware eID ne peut pas faire usage du lecteur de cartes pour la carte eID.

© 2006 SPF Technologie de l'Information et de la Communication (Fedict)

LES ÉLÉMENTS DU LOGICIEL EID

Maintenant que l'installation est réalisée, il est temps de faire connaissance avec les éléments essentiels du middleware eID.

- un module d'extension (plug-in) PKCS#11 (libbeidpkcs11.so) qui permet d'utiliser la carte d'identité pour authentifier une signature électronique
- une application (beidgui) pour lire, contrôler, imprimer et sauvegarder dans un fichier le contenu de la carte d'identité
- quelques command line tools (beid-tool et beid-pkcs11-tool)

S'y ajoutent encore deux éléments non visibles ou "daemons", en charge de l'exécution de tâches de fond en arrière-plan telles que le contrôle des applications qui essaient de lire la carte eID.

© 2006 SPF Technologie de l'Information et de la Communication (Fedict)

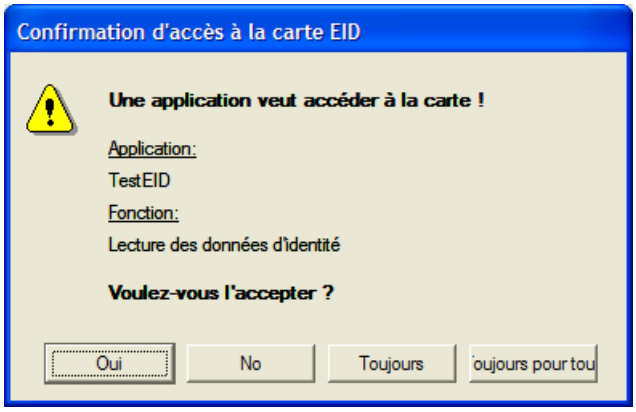
LE FILTRE VIE PRIVÉE

Cette option n'est disponible que si la configuration du script d'initialisation (init script) et du niveau d'exécution (runlevel) est correcte.

Le filtre vie privée est un composant invisible qui surveille toute communication avec la carte eID à la manière d'un chien de garde.

Lorsque le filtre vie privée est actif, seuls les programmes qui sont développés à l'aide du logiciel officiel produit par le gouvernement peuvent faire usage de la carte eID.

En outre, le filtre vie privée affichera un avertissement à chaque fois qu'un programme inconnu essaie de lire les données d'une carte eID.



Le filtre vie privée fournit les informations suivantes:

- nom du programme qui essaie de lire la carte
- fichier de données à lire (adresse, identité ou photo)

L'utilisateur peut décider lui-même s'il autorise ce programme à lire la carte d'identité:

- oui (uniquement cette fois-ci)
- non
- toujours (pour ce programme)
- toujours pour tout (pour tous les programmes)

Note: le filtre vie privée est un daemon (beidpcscd) qui est lancé via un runlevel init script dans /etc/init.d.

CONFLIT AVEC LE PARE-FEU PERSONNEL

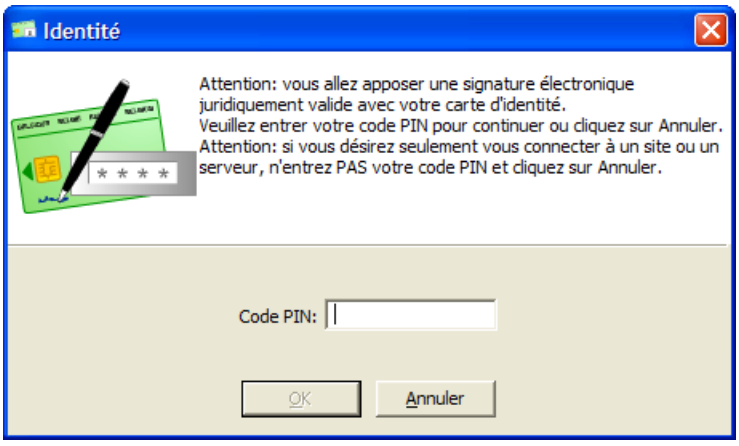
Pour permettre aux différents éléments du middleware eID de

communiquer avec le filtre vie privée, il est parfois nécessaire de configurer le pare-feu personnel de façon à autoriser la communication via l'adresse IP 127.0.0.1 ou le nom d'hôte "localhost" et le numéro de port TCP 2500. Cette adresse n'est toutefois pas une véritable adresse Internet mais une adresse virtuelle qui signifie “l'ordinateur local”.

LE MODULE PKCS#11

Il ne s'agit pas ici d'un logiciel autonome que vous pouvez lancer vous-même mais d'un module qui est utilisés par d'autres programmes pour communiquer avec la carte eID.

Ces modules demeurent invisibles sauf lorsque vous devez introduire votre code PIN, par exemple pour accéder à un site Web ou pour signer un document.


Identité
Attention: vous allez apposer une signature électronique juridiquement valide avec votre carte d'identité.
Veuillez entrer votre code PIN pour continuer ou cliquez sur Annuler.
Attention: si vous désirez seulement vous connecter à un site ou un serveur, n'entrez PAS votre code PIN et cliquez sur Annuler.
* * * *
Code PIN:
OK
Annuler

Le module PKCS#11 est une librairie partagée appelée libbeidpkcs11.so. Le répertoire dans lequel cette librairie est installée dépend de la distribution et des options de construction dans le cas d'une installation à partir du code source. Le plus souvent ce fichier se trouve dans /usr/local/lib ou dans /usr/lib.

Quelques applications utilisant le module PKCS#11:

- Firefox
- Thunderbird
- Mozilla et Netscape
- Lotus Notes

La configuration et l'utilisation de ces applications avec la carte eID sont décrites dans d'autres manuels.

APPLICATION POUR LIRE ET CONTRÔLER LA CARTE

L'application peut être lancée via l'icône sur le bureau, via le menu Start ou via la ligne de commandes (beidgui):

Cette application n'est disponible que si wxWidgets (wxGtk) est installé.

```
# beid-gui &
```

L'application propose 4 écrans d'information, respectivement pour les données d'identité, les certificats, le statut de la carte et du code PIN et les options du programme.

L'ÉCRAN "IDENTITÉ"

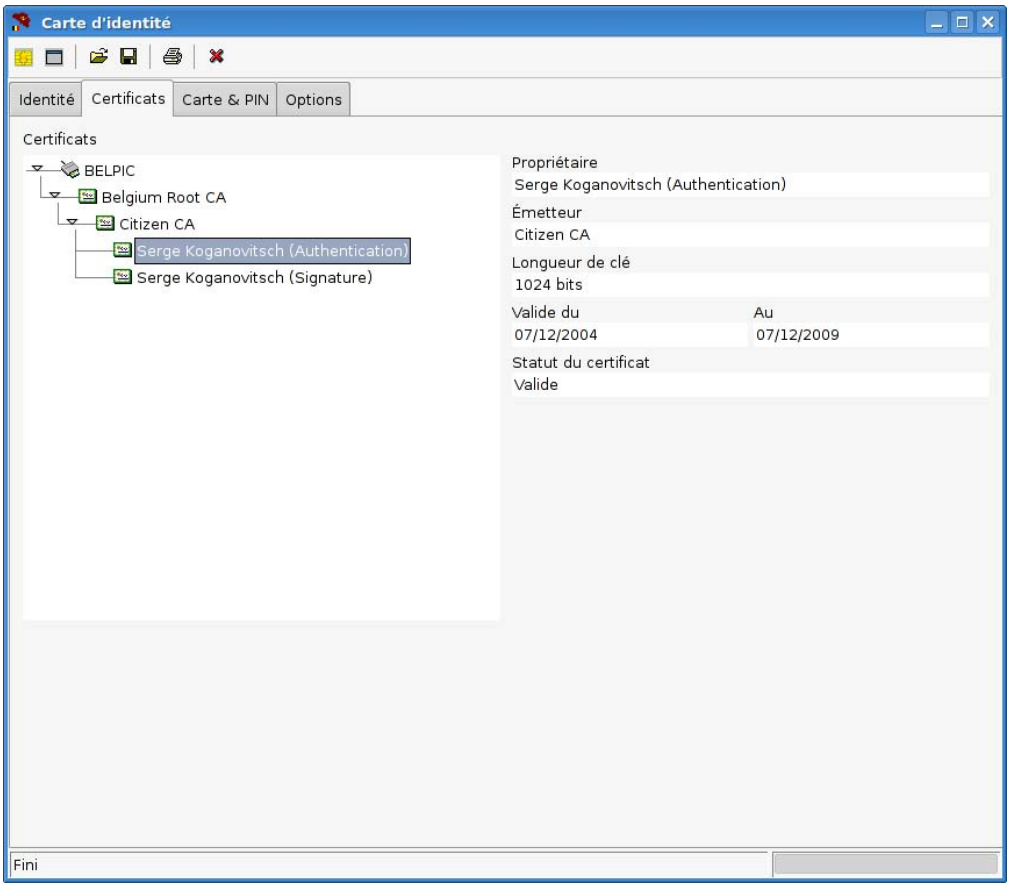
Outre les données d'identité, l'adresse et la photo, cet écran fournit également l'information sur la période de validité, le numéro de série de la puce et le statut spécial éventuel du détenteur.

L'ÉCRAN "CERTIFICATS"

Une carte eID peut être parfaitement valable alors même que un ou plusieurs certificats sont rejetés. Le statut d'un certificat est indépendant du statut de la carte gérée.

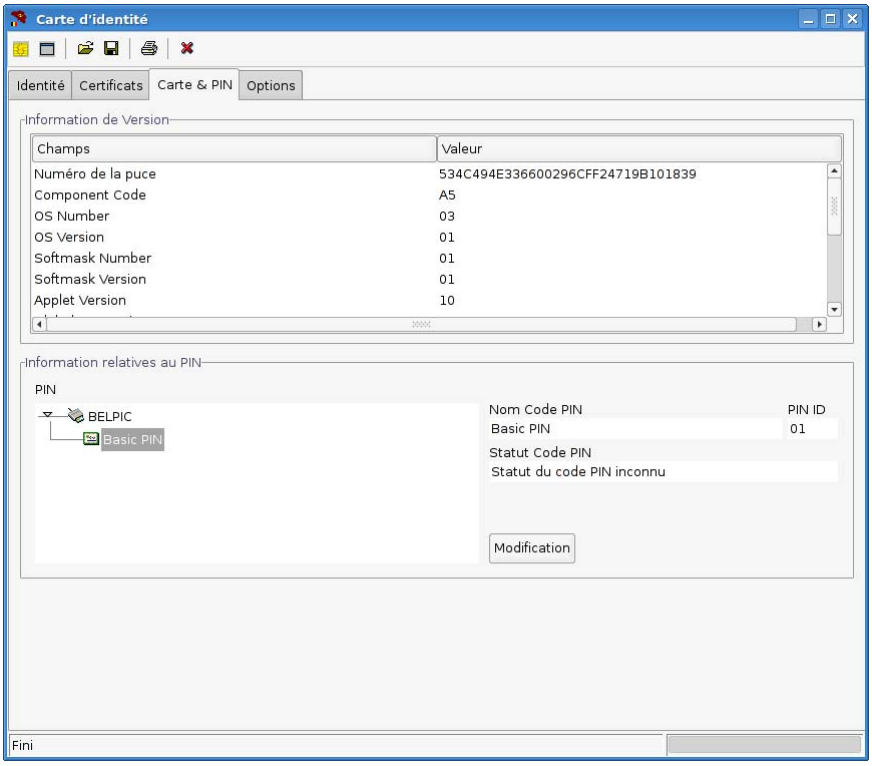
Cet écran affiche dans sa partie gauche les certificats qui figurent dans la carte. Chaque certificat peut être sélectionné individuellement pour en consulter le statut dans la partie droite de l'écran. Le statut des certificats peut être le suivant:

- valable
- expiré
- temporairement rejeté
- définitivement rejeté



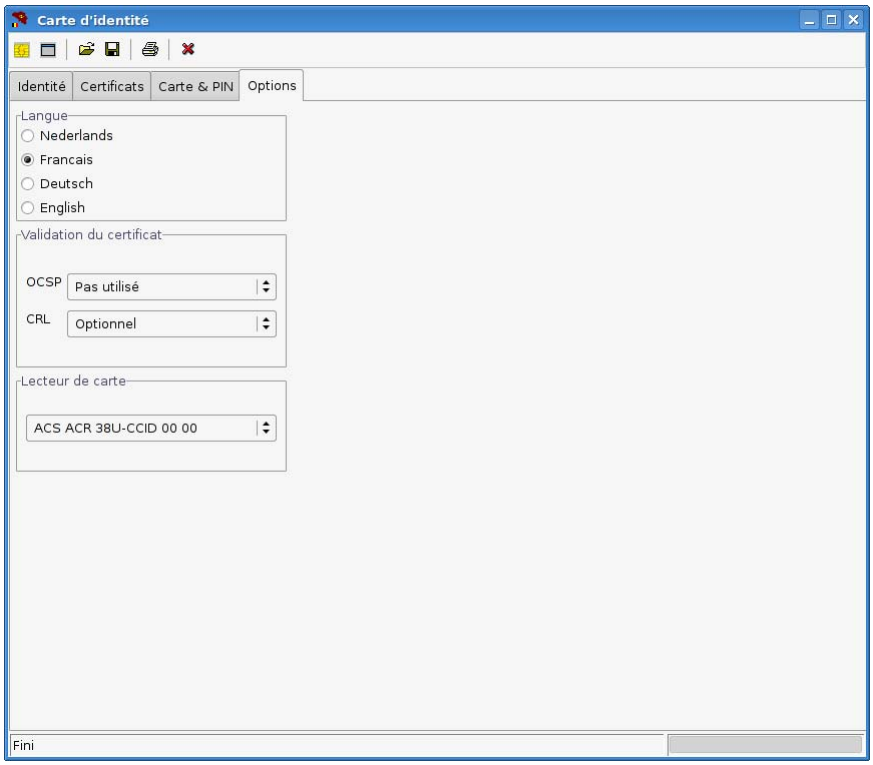
L'ÉCRAN "CARTE ET PIN"

Cet écran affiche l'information sur la puce et offre la possibilité de modifier le code PIN.



L'ÉCRAN "OPTIONS"

Cet écran reprend les options générales du programme.



Langue:

Le choix de langue s'applique uniquement à ce programme et n'a pas d'influence sur le langage utilisé par d'autres applications.

Validité du certificat:

Comme déjà indiqué, les certificats sur la carte peuvent être valides, expirés ou rejetés. Pour vérifier leur état actuel, le programme va contrôler en ligne le statut des certificats au cas par cas (option OCSP ou Online Certificate Status Protocol) ou télécharger périodiquement une nouvelle liste des certificats rejetés (option CRL of Certificate Revocation List).

Pour chacun de ces deux mécanismes de contrôle, il est possible d'indiquer la marche à suivre:

- *Non utilisé:* ce contrôle ne sera jamais effectué
- *Optionnel:* la méthode est utilisée si les circonstances le permettent. Ainsi, dans le cas d'un contrôle par OCSP, il faut qu'une connexion Internet soit disponible au moment de la

vérification des certificats. Pour un contrôle par CRL, l'ordinateur doit être en possession d'une version actualisée de la liste CRL ou – au cas où la liste locale n'est plus d'actualité – disposer d'une connexion Internet pour télécharger une nouvelle liste.

- *Obligatoire:* si une méthode de contrôle est imposée mais ne peut pas être appliquée (faute de connexion Internet, par exemple), un message d'erreur apparaît et les données de la carte ne sont pas montrées.

Lecteur de cartes:

Si aucun lecteur de carte n'est spécifié, le programme va examiner tous les lecteurs de carte disponibles et lire la première carte eID qu'il trouvera. Si vous le souhaitez, vous pouvez sélectionner ici un lecteur de carte spécifique à partir de la liste affichée qui contient tous les lecteurs de carte connectés pour l'heure.

LES OUTILS DE LA LIGNE DE COMMANDES

BEID-TOOL

La commande *beid-tool* montre tous les lecteurs de cartes connectés et le code de réponse des cartes insérées dans ces lecteurs.

Détection du lecteur de cartes:

```
# beid-tool -l
Readers known about:
Nr.    Driver     Name
0      pcsc       ACS ACR38U 00 00
```

Détection de la carte eID:

```
# beid-tool -a
Connecting to card in reader ACS ACR38 00 00
Using card driver: BE eID card
Card ATR: 3B 98 94 40 0A A5 03 01 01 01 AD 13 10
;..@.........
```

BEID-PKCS11-TOOL

La commande *beid-tool* teste les fonctions cryptographiques de la carte.

Test de la carte eID:

```
# beid-pkcs11-tool -t -l --module
/usr/local/lib/libbeidpkcs11.so
```

Daemons et Init Scripts

Le middleware eID comprend deux daemons (démons):

1. le daemon beidpcscd pour le filtre vie privée
2. le daemon beidcrld pour le téléchargement périodique de la liste CRL

Le répertoire dans lequel ces daemons sont installés dépend de la distribution et des options de construction dans le cas d'une installation à partir du code source. Le plus souvent ce fichier se trouve dans /usr/local/bin ou dans /usr/bin.

Les daemons sont lancés via des scripts init dans /etc/init.d:

- belgium.be-beidpcscd pour beidpcscd
- belgium.be-beidcrld pour beidcrld

Dans la plupart des distributions, la base de noyau (core package) LSB est disponible mais pas installée.

Les scripts livrés avec le code source sont conformes aux standards "Linux Standard Base" v3.1. Pour un fonctionnement correct de ces scripts la base de noyau (core package) LSB doit également être installée pour votre distribution.

Un tuyau: lorsque la base de noyau LSB est installée pour votre distribution, les trois fichiers suivants se trouvent disponibles:

- /lib/lsb/init-functions
- /usr/lib/lsb/install_initd
- /usr/lib/lsb/remove_initd.

Enregistrement des scripts init après installation par l'intermédiaire du code source standard:

Après l'installation au moyen de make install, les scripts init doivent encore être enregistrés de façon à ce que les daemons soient lancés dans les bons niveaux d'exécution (runlevels). Ceci peut se faire par l'enregistrement des scripts en tant que root avec la commande install_initd.

Dans certaines distributions, il faut parfois utiliser une commande de distribution spécifique au lieu de la commande LSB install_initd.

Il est également possible que des distributions aient adapté ces scripts et que la base de noyau LSB ne soit pas nécessaire.

© 2006 SPF Technologie de l'Information et de la Communication (Fedict)

---------- Ceci est la dernière page du document ----------

© 2006 SPF Technologie de l'Information et de la Communication (Fedict)